МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.60797/IRJ.2024.144.110

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ ИНТЕРНЕТА ВЕЩЕЙ И СПОСОБЫ ЗАЩИТЫ ОТ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ IOT

Научная статья

Осипов Д.С.[1,] *, Малахов С.В.[2], Якупов Д.О.[3], Храмова А.Е.[4], Крючкова А.С.[5], Джакимова А.Т.[6]

[2] ORCID : 0009-0001-8666-6713;

[3] ORCID : 0009-0003-2371-0822;

[1, 2, 3, 4, 5, 6] Поволжский государственный университет телекоммуникации и информатики, Самара, Российская Федерация

* Корреспондирующий автор (daniil.osipov38[at]gmail.com)

Аннотация

В статье описывается оценка существующих угроз и уязвимостей в системах Интернета Вещей, а также разработка рекомендаций и стратегий по их минимизации. В рамках исследования проанализирована обстановка в области безопасности Интернета Вещей, выявлены основные угрозы и риски, и предложены практические подходы к решению существующих проблем. Работа предоставляет ценные идеи и рекомендации для будущих исследовательских и развивающихся деятельностей в области умных устройств. Информация в статье способствует развитию методов обнаружения аномалий, дополнительно улучшая безопасность и надежность Интернета Вещей. Результаты исследования могут быть полезны для специалистов в области информационной безопасности, разработчиков устройств для Интернета вещей, а также для организаций, занимающихся их внедрением и эксплуатацией.

Ключевые слова: Интернет Вещей, сеть, данные, аномалия, машинное обучение, безопасность.

DETECTING INTERNET OF THINGS VULNERABILITIES AND WAYS TO PROTECT AGAINST AN IOT INFORMATION SECURITY BREACH

Research article

Osipov D.S.[1,] *, Malakhov S.V.[2], Yakupov D.O.[3], Khramova A.Y.[4], Kryuchkova A.S.[5], Dzhakimova A.T.[6]

[2] ORCID : 0009-0001-8666-6713;

[3] ORCID : 0009-0003-2371-0822;

[1, 2, 3, 4, 5, 6] Povolzhskiy State University of Telecommunications and Informatics, Samara, Russian Federation

* Corresponding author (daniil.osipov38[at]gmail.com)

Abstract

The article describes the evaluation of existing threats and vulnerabilities in Internet of Things systems, as well as the development of recommendations and strategies to minimize them. The research analyses the Internet of Things security environment, identifies the main threats and risks, and proposes practical approaches to address the existing challenges. The work provides valuable insights and recommendations for future research and development activities in the field of smart devices. The information in the work contributes to the development of anomaly detection techniques, further improving the security and reliability of the Internet of Things. The results of the research can be useful for information security professionals, developers of devices for the Internet of Things, and organizations involved in their implementation and operation.

Keywords: Internet of Things, network, data, anomaly, machine learning, security.

Введение

В настоящее время Интернет Вещей (IoT) – это широко распространенный термин в области будущих технологий. IoT представляет собой сеть, состоящую из умных объектов [1]. Эти узлы играют ключевую роль в сети Интернета Вещей, обеспечивая обмен информацией и связь между пользователями [1]. Интернет вещей считается основой текущего расширения интернет-сервисов, позволяющей охватить все различные формы объектов.

У сетей Интернета Вещей есть большие проблемы с безопасностью. Некоторые из них могут быть вызваны атакой на различные уровни архитектуры Интернета Вещей, в то время как другие атаки могут быть вызваны проникновением хакера в сеть и взлома сетевых компонентов с целью их ослабления.

Вопросы, связанные с обнаружением аномалий в компьютерных сетях и в сети Интернета вещей, интересуют специалистов в области компьютерной безопасности достаточно давно. Многие работы посвящены обзору state-of-the-art в детектировании аномалий [2], [3], [5], [6], [7]. В них предлагаются различные схемы классификации как самих атак, так и методов, и средств их обнаружения.

Несмотря на то, что во многих случаях успешно ведут себя статистические методы обнаружения сетевых атак [8], большинство исследователей считают, что наибольшей эффективностью по обнаружению аномалий в современных компьютерных сетях, учитывая сложность, распределённость и интегрированность формируемых на их основе информационных инфраструктур, обладают методы машинного обучения [9], [10].

Методы машинного обучения могут существенно повысить эффективность и снизить трудоемкость решения задач компьютерной безопасности в современных цифровых сетях. Так, в [11] показано, что наибольшей популярностью

среди методов машинного обучения по обнаружению компьютерных атак обладают SVM (Support Vector Machine) алгоритмы. Эти методы в различных условиях обеспечивают точность в диапазоне от 80 до 99.6%.

Одним из направлений повышения эффективности обнаружения аномалий с помощью методов машинного обучения является эффективное комбинирование различных методов.

В работе рассматривается комплексный подход к обнаружению уязвимостей в IoT, который включает в себя использование машинного обучения, деревьев решений, криптографических и физических методов защиты. Это позволит создать более надежную и эффективную систему обнаружения уязвимостей, способную адаптироваться к постоянно меняющемуся ландшафту угроз безопасности IoT.

Основная часть

Независимо от варианта использования, системы Интернета Вещей включают в себя одни и те же четыре компонента (см. рис. 1): устройства, подключенные шлюзы, платформы и приложения [12]. Все четыре компонента составляют основу решения, но количество уровней может варьироваться в зависимости от варианта использования Интернета Вещей.

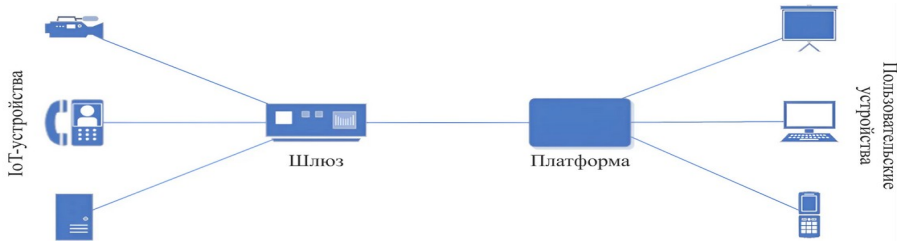

Рисунок 1 - Основа архитектуры устройств Интернета Вещей
DOI: https://doi.org/10.60797/IRJ.2024.144.110.1

Существуют ключевые элементы в обеспечении безопасности IoT. Проактивная защита и адаптивные технологии являются ключевыми элементами в обеспечении безопасности IoT. Разработчики и производители должны внедрять сложные алгоритмы шифрования и многоуровневые системы аутентификации. Также критически важно обновлять программное обеспечение и прошивки устройств для защиты от новейших угроз.

Не менее важным является образование конечных пользователей. Люди должны быть информированы о потенциальных рисках и лучших практиках использования IoT-устройств. Это включает в себя регулярное изменение паролей, использование двухфакторной аутентификации и избегание подключения к незащищенным сетям Wi-Fi [13].

В реальных наборах данных существуют случаи, которые отличаются от всех остальных и признаются аномалиями. Определение аномалий заключается в обнаружении явлений, которые считаются необычными по сравнению с нормальными событиями. Обнаружение аномалий находит применение в различных областях Интернета Вещей (IoT), включая умные города, сетевую безопасность и промышленность. Это важный инструмент для выявления нештатных ситуаций и обеспечения более эффективного управления системами. Алгоритмы обнаружения аномалий могут быть применены также в медицинских исследованиях, финансовой аналитике и других областях, где важно выявление редких и необычных событий. Ключевые уязвимости безопасности:

- Системы обнаружения вторжений: устройства IoT подключены к Интернету и продолжают оставаться уязвимыми для атак, связанных с безопасностью. Угрозы, такие как атаки DoS и DDoS, наносят значительный ущерб сети IoT.

- Распознавание фрода: При подключении к системе или выполнении онлайн-транзакций, IoT-сети подвержены риску перехвата конфиденциальных данных, включая информацию о кредитных картах и банковские сведения [14].

- Защита от потери данных: Важная информация может утекать из корпоративных баз данных и серверов, создавая риски для безопасности и конфиденциальности. Эффективное использование методов шифрования может помочь предотвратить такие инциденты.

Аномалии могут быть обнаружены разными способами:

Точечные аномалии: Когда эволюция последовательности непредсказуема, аномалии используются для выявления значительно отличающихся точек от остальных данных. Этот метод часто используется для обнаружения мошенничества.

Коллективные аномалии: Наблюдаются типичные временные ряды, такие как повторяющиеся паттерны или формы от множества устройств IoT. Например, в случае задержек в поставке в цепи поставок требуется аудит и совместный анализ при множественных задержках [15].

Контекстные аномалии: Обнаруживаются, когда учитывается предварительный тип или значение, такие как день недели. Контексты очень обширны и зависят от конкретной области.

Ключевыми методами защиты от аномалий являются методы машинного обучения, криптографические и физические методы защиты.

Начнем с методов машинного обучения по определению аномалий в IoT. Структура обнаружения аномалий для Интернета Вещей с помощью машинного обучения состоит из трех этапов: этап предварительной обработки, этап выбора функций и этап классификации [16].

Этап предварительной обработки. Этап очистки и структурирования данных является наиболее важной частью этапа предварительной обработки. Очистка данных удаляет дубликаты, заменяет недостающие данные, исправляет

структурные ошибки и удаляет нежелательные наблюдения. После очистки данные стандартизируются по следующей формуле:

$$x_{std}^{(i)} = \frac{x^i - \mu^x}{\sigma_x},$$

где x – значение данных, μ – среднее значение данных, а – σ дисперсия данных.

Этап выбора функции. Функции сбора данных является наиболее важным шагом в опознавании аномалий. Чтобы создать эффективные, действенные, а также простые модели обнаружения, необходимо выбрать наиболее важные признаки. Оптимально подобранные представления признаков приводят к созданию полезных моделей прогнозирования [17]. Цели выбора признаков – сократить объем данных для подгонки, повысить точность обнаружения и минимизировать время обнаружения [17]. Такие надежные модели прогнозирования должны быстро обнаруживать атаки до того, как они нанесут дальнейший ущерб системе. Кроме того, IoT-устройства требуют упрощенных методов обнаружения аномалий из-за ограниченных вычислительных ресурсов. Поэтому для выбора наиболее значимых признаков для метода обнаружения используется модель совместного машинного обучения. Данный подход позволяет эффективно прогнозировать атаки с высокой точностью и коротким временем обнаружения. Он основан на наборе моделей машинного обучения, которые совместно выбирают наилучшие дискриминационные признаки и отсеивают бесполезные. В данном контексте рекомендуется использовать четыре метода машинного обучения. Деревья решений (DT) – метод, который строит дерево, разбивая данные на более мелкие группы на основе признаков. Он может быть эффективен в выявлении важных характеристик. Дополнительные деревья (ET) – метод также использует деревья решений, но строит их в виде набора данных. Он устойчив к переобучению и может помочь в отборе признаков. Случайный лес (RF) также является набором деревьев решений. Он обучает несколько деревьев на разных подмножествах данных и усредняет их предсказания. Это помогает в выявлении важных признаков. XGBoost (XGB) – градиентный бустинг, который также использует набор деревьев. Он эффективен в решении задач классификации и регрессии, а также может помочь в отборе признаков.

Каждый метод отбора признаков самостоятельно определяет лучшие признаки на основе эффективности обнаружения, а высокорезультативные признаки добавляются в оптимальный набор признаков и используются на этапе обнаружения.

Деревья принятия решений (DT) представляют собой древовидную структуру, аналогичную блок-схеме. Внутренние узлы этой структуры представляют объекты или атрибуты ветви - правила принятия решений, а каждый конечный узел – результат [17]. В DT корневой узел выполняет разбиение на основе значений атрибутов. Рекурсивное разбиение - это метод, который точно отражает мыслительные процессы человека и полезен для принятия решений. DT требует меньше времени на подготовку данных, чем другие методы, и его временная сложность зависит от количества записей и признаков в предоставленных данных. Кроме того, DT – это непараметрический подход, не зависящий от предположений о распределении и вероятностных распределениях.

Преимущества использования деревьев принятия решений:

1. Интерпретируемость: DT легко интерпретировать, поскольку они представляются в виде деревьев с понятными ветвями и узлами.

2. Малая подготовка данных: DT не требуют сложной предобработки данных, так как они могут обрабатывать категориальные и числовые признаки без дополнительных преобразований.

3. Устойчивость к выбросам: DT менее чувствительны к выбросам в данных, чем некоторые другие методы.

4. Автоматический отбор признаков: DT могут автоматически выбирать наиболее важные признаки для принятия решений.

5. Обработка пропущенных значений: DT могут обрабатывать пропущенные значения в данных.

6. Масштабируемость: DT могут обрабатывать большие объемы данных.

В основе всех алгоритмов построения дерева решений лежат следующие базовые принципы

· Для разделения записи выбирается наиболее подходящий атрибут с помощью критерия выбора атрибутов (ASM).

· Используя этот атрибут в качестве узла принятия решения, набор информации разбивается на мелкие подмножества.

· Начните строить дерево, повторяя этот метод для каждого дочернего элемента до тех пор, пока не будет выполнено одно из следующих условий:

1. Все кортежи объединены с одним и тем же значением атрибута.

2. Больше нет доступных атрибутов.

3. Больше нет примеров.

Метод *Gini* используется для получения точек разделения в алгоритме дерева решений

$$Gini(D) = 1 - \sum_{i=1}^{m} \pi\lambda^2.$$

Если данные D разделены на D1 и D2 в результате двоичного разделения по атрибуту A, индекс *Gini* является:

$$Gini_A(D) = \frac{|D_1|}{|D|} Gini(D_1) + \frac{|D_2|}{|D|} Gini(D_2).$$

Далее идет выбор подмножества, которое обеспечивает самое маленькое значение Джини. Если речь идет о непрерывных признаках, то следует рассматривать пары значений как потенциальный момент разделения и выбираем тот, который имеет самый маленький коэффициент Gini.

$$\Delta Gini(A) = Gini(D) - Gini_A(D).$$

Атрибут с наименьшим индексом *Gini* выбирается в качестве разделяющего атрибута.

2.1. Деревья с высокой степенью рандомизации (ET)

ET – это вид метода машинного обучения, который предоставляет итоги классификации путем объединения всех результатов набора некоррелированных деревьев решений, собранных в «лес», но метод создания деревьев решений отличается тем, что в решениях деревьев с высокой степенью рандомизации исходные обучающие выборки

используются для генерации всех деревьев, используемых для создания деревьев. После этого каждому тестовому узлу дерева дается случайная подборка k функций из общего набора функций. Из них оно должно выбрать лучший пример для сортировки данных в сопоставлении с математическим критерием (обычно это индекс *Gini*) [17]. Эта подборка признаков используется для выстраивания ряда декорреляционных деревьев решений. После создания леса посчитанные нормализационные сокращения используются при принятии решений об объектах (индекс *Gini* используется при создании леса), вычисляется, и для каждого признака производится отбор с использованием структуры леса, описанной выше. Важность признака Джини определяется именем, присвоенным его значению. При выборе признаков каждый признак ранжируется в порядке убывания важности в соответствии с индексом Джини, и пользователь выбирает k лучших признаков в соответствии со своими предпочтениями:

$$Gini = 1 - \sum_{i=1}^{C} \pi^2,$$

где C общее количество классов и π это вероятность того, что элемент будет классифицирован как принадлежащий определенному классу.

Случайный лес (Random Forest, RF) – это метод машинного обучения, который использует массив деревьев решений. Модель случайного леса создает несколько деревьев решений на основе случайной выборки из обучающих данных. Каждое дерево строится независимо друг от друга. Когда необходимо сделать прогноз для нового объекта, каждое дерево вносит свой вклад. Голоса всех деревьев агрегируются для формирования окончательного прогноза.

Для определения важности признаков случайный лес использует уменьшение примеси узла (например, Gini impurity или энтропия). Вероятность достижения узла рассчитывается как отношение числа экземпляров, дошедших до этого узла, к общему числу экземпляров. Чем выше вклад признака в уменьшение примеси, тем важнее этот признак для модели.

Преимущества случайного леса включают:

- Хорошую обобщающую способность: RF способен обучаться на разнообразных данных и давать точные прогнозы.

- Устойчивость к переобучению: Благодаря агрегации нескольких деревьев, случайный лес менее подвержен переобучению.

- Обработку больших объемов данных: RF может обрабатывать большие наборы данных.

Однако случайный лес также может быть чувствительным к шуму и требовать больше ресурсов для обучения, чем одиночные деревья решений. Значения индекса Джини используются для оценки важности каждого узла в дереве решений, предполагающем только два дочерних узла (бинарное дерево).

$$ni_j = \omega_j C_j - \omega_{left(j)} C_{left(j)} - \omega_{right(j)} C_{right(j)},$$

где взвешенное количество выборок в узле *j* как часть общего взвешенного количества выборок, *j* – примесь в узле, а *left(j)* и *right(j)* – соответствующие дочерние узлы.

2.2. XGBoost

Метод предоставляет поиск разделения для оптимизации деревьев, а также встроенную регуляризацию для предотвращения переобучения. В целом, XGBoost – это более быстрая и точная форма повышения градиента. Основной принцип метода XGBoost заключается в постепенном обучении модели дерева ансамбля (группы) с использованием штрафного параметра.

2.3. Метод выбора функций

Дано задание на классификацию и набор обучающих примеров (x_i,y_i), в которых $x_i \in \mathbb{R}^n$ является исходным примером и $y_i \in \{-1, 1\}$ соответствует классу и $1 \le i \le n$ наша основная задача – выбрать набор функций f_k, таких , что $k \le n$ на основе поиска классификатора с функцией принятия решения f_k (X, θ) таких, что вектор класса маркировки Y это функция$Y=f_k$ (X,θ) и θ представляет собой набор параметров, которые определяются в соответствии с некоторым классификатором ∈{DT, ET, RF, XGB} [17]. Для определения локальной значимости каждой переменной в признаке мы анализируем параметры используемого классификатора и применяем общую важность объекта. На этапе выбора признаков применяются различные методы машинного обучения для выявления наилучших характеристик из заданного набора данных. В этот момент также предлагаются новые методы отбора наиболее важных признаков, содержащих критические данные, которые могут быть использованы для создания модели обнаружения аномалий [17].

На этапе анализа признаков в машинном обучении, помимо оценки важности переменных, также рассматриваются различные методы отбора признаков. Метод отбора на основе важности использует параметры классификатора (например, случайного леса или градиентного бустинга), чтобы определить, какие признаки оказывают наибольшее влияние на целевую переменную. После этого можно выбрать наиболее важные признаки для дальнейшего анализа.

Рекурсивное исключение признаков (RFE): RFE начинает с полного набора признаков и последовательно исключает наименее важные. Этот процесс повторяется до тех пор, пока не останется заданное количество наиболее важных признаков.

Методы отбора на основе статистики используют статистические метрики, такие как корреляция или анализ дисперсии, чтобы определить, какие признаки наиболее информативны для модели.

Отбор на основе рекурсивной элиминации (RFE) начинает с полного набора признаков и последовательно удаляет наименее важные. Он продолжает этот процесс до тех пор, пока не останется заданное количество наиболее важных признаков.

Методы отбора на основе L1-регуляризации штрафуют модель за большое количество признаков, что позволяет автоматически отбирать наиболее важные.

Предлагается применить все методы машинного обучения (DT, ET, RF, XGB) и выбрать признаки с наилучшей тройкой признаков (Ac, Pr, Fs) по следующей формуле:

$$f_k = max(Ac, Pr, Fs)_r^{C^i}{}_{i=1..N},$$

где N – количество классификаторов, Ac, Pr обозначает значение точности, Fs – среднее значение точности измерений, C^i – набор используемых классификаторов [17].

2.4. Криптографические методы защиты

В этом методе используются математические алгоритмы для обеспечения конфиденциальности, целостности и подлинности информации. В сетях IoT, где данные часто передаются по открытым каналам связи, криптографические методы играют важную роль в обеспечении безопасности [18].

Шифрование трафика позволяет скрыть содержимое передаваемых данных от несанкционированного доступа. Это достигается путем применения криптографических алгоритмов шифрования к данным перед их передачей по сети. Расшифровать данные могут только авторизованные пользователи, имеющие соответствующие ключи доступа.

Аутентификация устройств и пользователей гарантирует, что только доверенные лица могут получить доступ к данным и ресурсам в системах IoT. Этого можно достичь с помощью таких протоколов аутентификации, как HMAC и цифровые сертификаты, которые проверяют личность пользователей и устройств.

Криптографические методы защиты данных обеспечивают высокий уровень безопасности и конфиденциальности данных в сетях IoT. Они обеспечивают защиту от атак хэширования и репликации, а также предотвращают перехват и модификацию данных. Однако они могут потреблять дополнительную вычислительную мощность и вызывать задержки при передаче данных [19]. Кроме того, эффективность криптографических методов зависит от правильного управления ключами и реализации протоколов безопасности.

2.5. Физические методы защиты

Обеспечение безопасности устройств IoT включает в себя выбор надежных и соответствующих стандартам устройств, непрерывный мониторинг и наличие компетентной сетевой инфраструктуры безопасности. Но также важна и хорошо известная физическая безопасность [20]. Не должно быть такого, чтобы за безопасность инфраструктуры IoT отвечала только одна группа кибербезопасности. Необходимо устанавливать сотрудничество и общую ответственность между командами по кибербезопасности, операционной деятельности и управления, а также физической безопасности. Участие всех трех сторон обеспечит лучший результат.

- Следует удалить любые средства подключения – оптические порты, радиоустройства – которые существуют исключительно в целях разработки. Кроме того, с учетом структуры и назначения устройств, необходимо удаление всех точек тестирования или отключение тестового доступа, а также защита устройств от несанкционированного цифрового доступа. Любой вид тестового или административного доступа, скорее всего, станет целью для атакующих [21].

- Все устройства должны находиться в режиме эксплуатации и не находиться в режимах настройки по умолчанию, сброса или парного режима.

- Должны использоваться устройства, которые обеспечивают защиту от физического вмешательства.

- Обучение сотрудников распознаванию и предотвращению атак методом социальной инженерии, которые могут быть использованы злоумышленниками для получения доступа к ограниченным зонам, где установлены устройства IoT [22].

- Все устройства IoT должны быть защищены от огня, воды, механических повреждений и вандализма.

Хотя устройства IoT превосходно подходят для мониторинга объектов, необходимо убедиться, что сами устройства контролируются подходящими системами, которые обнаруживают несанкционированный доступ и вмешательство, потому что обнаружение физических угроз безопасности труднее всего обнаружить в сети IoT.

Заключение

В работе рассмотрены методы защиты для обнаружения аномалий в сетевом поведении устройств Интернета Вещей, а именно методы машинного обучения, криптографические методы и физические методы защиты. Проанализировано, что данные методики способны обнаружить как угрозы физической безопасности, так и аномалии в трафике данных, поскольку соответствующие оценки угрозы для обеих атак были ниже уровня безопасности. В рамках исследования были проанализированы различные методы обнаружения уязвимостей и защиты данных в IoT, что позволяет получить более полное представление о возможностях и ограничениях каждого из этих методов. Это, в свою очередь, позволяет определить наиболее эффективные стратегии защиты для различных типов IoT-устройств и сценариев использования. В ходе будущей работы будут проводиться эксперименты, чтобы протестировать и разработать комбинированную методологию обнаружения атак. Более того, будут проведены эксперименты с использованием кластеризации для определения общих характеристик и поведения устройств в IoT системе, что может помочь в управлении и мониторинге системы.

Конфликт интересов

Не указан.

Рецензия

Артамонов В.А., Международная академия информационных технологий (МНОО "МАИТ), Минск, Беларусь

DOI: https://doi.org/10.60797/IRJ.2024.144.110.2

Conflict of Interest

None declared.

Review

Артамонов V.A., International Academy of information technologies, Minsk, Belarus

DOI: https://doi.org/10.60797/IRJ.2024.144.110.2

Список литературы / References

1. Dhuha K.A. A Review on Security and Privacy Issues and Challenges in Internet of Things / K.A. Dhuha, N.Z. Jhanjh // International Journal of Computer Science and Network Security. — 2020. — 20.

2. Raimundo M. Application of Hurst Exponent (H) and the R/S Analysis in the Classification of FOREX Securities / M. Raimundo, Jr. Okamoto // International Journal of Modeling and Optimization. — 2018. — 8. — p. 116–124.

3. Sánchez-Granero M. Introducing fractal dimension algorithms to calculate the Hurst exponent of financial time series / M. Sánchez-Granero, M. Fernández-Martínez, J. Trinidad-Segovia // European Physical Journal B. — 2012. — 85. — p. 86.

4. Grillo D. Personal Communication Services and Teletraffic Standardization in ITU-T. In The Fundamental Role of Teletraffic in the Evolution of Telecommunications Networks, Proceedings of the 14th International Teletraffic Congress - ITC 14, Antibes Juan-les-Pins / D. Grillo, A. Lewis, R. Pandya // Elsevier Science. — 1994. — 1. — p. 1-12.

5. Strelkovskaya I. Spline-Extrapolation Method in Traffic Forecasting in 5G Networks / I. Strelkovskaya, I. Solovskaya, A. Makoganiuk // Journal of Telecommunications and Information Technology. — 2019. — 3. — p. 8-16.

6. Carvalho P. Analysis of the influence of self-similar traffic in the performance of real time applications / P. Carvalho, H. Abdalla, A. Soares et al. — 2005 — URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.599.4041&rep=rep1&type=pdf (accessed: 11.06.2024)

7. Ruoyu Ya. Hurst Parameter for Security Evaluation of LAN Traffic / Ya. Ruoyu, Yi. Wang // Information Technology Journal. — 2012. — 11. — p. 269–275.

8. Ably P. Self-Similarity and long-range dependence through the wavelet lens / P. Ably, P. Flandrin, M. Taqqu et al. // Theory and Applications of Long Range Dependence. — 2002. — 1. — p. 345–379.

9. Минькович Т.В. Информационные технологии: понятийно-терминологический аспект / Т.В. Минькович // ОТО. — 2012. — 2. — с. 371–389.

10. Расторгуев С.В. Информационные операции в сети Интернет / С.В. Расторгуев, М.В. Литвиненко — Москва: Центр стратегических оценок и прогнозов, 2014. — 128 с.

11. Михайлов А. П. Модели информационной борьбы / А. П. Михайлов, Н. А. Маревцева // Математическое моделирование. — 2011. — 10. — с. 19-32.

12. Росляков А.В. Интернет вещей / А.В. Росляков, С.В. Ваняшин, А.Ю. Гребешков — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2015. — 135 с.

13. Рентюк В.К. Краткий путеводитель по беспроводным технологиям «Интернета вещей». Часть 2. Ближний радиус действия / В.К. Рентюк // Control Engineering Россия. — 2018. — 1.

14. Zhihao W. Towards IP geolocation with intermediate routers based on topology discovery / W. Zhihao, L. Hong, L. Qiang et al. // Cybersecurity. — 2019. — 2.

15. Saenko I. Abnormal traffic detection in networks of the internet of things based on fuzzy logical inference / I. Saenko, I. Kotenko // Institute of Electrical and Electronics Engineers Inc. — 2015. — 18.

16. Patap U. Average state estimation in presence of outliers / U. Patap, C. Canudas-de-Wit, F. Garin // IEEE Conference on Decision and Control (CDC). — 2020. — 59.

17. Alanazi M. Anomaly Detection for Internet of Things Cyberattacks / M. Alanazi, A. Aljuhani // Tech Science Press. — 2022. — 72(1).

18. Thilakarathne N.N. Security and Privacy Issues in IoT Environment / N.N. Thilakarathne // International Journal of Engineering and Management Research. — 2020. — 10(1).

19. Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things — Introduced 2016-05-31. — Italy: Request for Comments, 2016.— 61 p.

20. Jones M.B. Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages / M.B. Jones // Internet Engineering Task Force. — 2017. — RFC8230.

21. Dagle J.E. Cyber-physical system security of smart grids / J.E. Dagle // IEEE PES Innovative Smart Grid Technologies (ISGT). — 2012. — 1.

22. Довгаль В.А. Проблемы и задачи безопасности интеллектуальных сетей, основанных на Интернете Вещей / В.А. Довгаль, Д.В. Довгаль // Ежеквартальный рецензируемый, реферируемый научный журнал "Вестник АГУ". — 2017. — 4(211).

Список литературы на английском языке / References in English

1. Dhuha K.A. A Review on Security and Privacy Issues and Challenges in Internet of Things / K.A. Dhuha, N.Z. Jhanjh // International Journal of Computer Science and Network Security. — 2020. — 20.

2. Raimundo M. Application of Hurst Exponent (H) and the R/S Analysis in the Classification of FOREX Securities / M. Raimundo, Jr. Okamoto // International Journal of Modeling and Optimization. — 2018. — 8. — p. 116–124.

3. Sánchez-Granero M. Introducing fractal dimension algorithms to calculate the Hurst exponent of financial time series / M. Sánchez-Granero, M. Fernández-Martínez, J. Trinidad-Segovia // European Physical Journal B. — 2012. — 85. — p. 86.

4. Grillo D. Personal Communication Services and Teletraffic Standardization in ITU-T. In The Fundamental Role of Teletraffic in the Evolution of Telecommunications Networks, Proceedings of the 14th International Teletraffic Congress - ITC 14, Antibes Juan-les-Pins / D. Grillo, A. Lewis, R. Pandya // Elsevier Science. — 1994. — 1. — p. 1-12.

5. Strelkovskaya I. Spline-Extrapolation Method in Traffic Forecasting in 5G Networks / I. Strelkovskaya, I. Solovskaya, A. Makoganiuk // Journal of Telecommunications and Information Technology. — 2019. — 3. — p. 8-16.

6. Carvalho P. Analysis of the influence of self-similar traffic in the performance of real time applications / P. Carvalho, H. Abdalla, A. Soares et al. — 2005 — URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.599.4041&rep=rep1&type=pdf (accessed: 11.06.2024)

7. Ruoyu Ya. Hurst Parameter for Security Evaluation of LAN Traffic / Ya. Ruoyu, Yi. Wang // Information Technology Journal. — 2012. — 11. — p. 269–275.

8. Ably P. Self-Similarity and long-range dependence through the wavelet lens / P. Ably, P. Flandrin, M. Taqqu et al. // Theory and Applications of Long Range Dependence. — 2002. — 1. — p. 345–379.

9. Min'kovich T.V. Informatsionnye tehnologii: ponjatijno-terminologicheskij aspekt [Information technology: conceptual and terminological aspect] / T.V. Min'kovich // OTO. — 2012. — 2. — p. 371–389. [in Russian]

10. Rastorguev S.V. Informatsionnye operatsii v seti Internet [Information operations on the Internet] / S.V. Rastorguev, M.V. Litvinenko — Moskva: Center for Strategic Assessments and Forecasts, 2014. — 128 p. [in Russian]

11. Mihajlov A. P. Modeli informatsionnoj bor'by [Models of information warfare] / A. P. Mihajlov, N. A. Marevtseva // Mathematical modeling. — 2011. — 10. — p. 19-32. [in Russian]

12. Rosljakov A.V. Internet veschej [Internet of Things] / A.V. Rosljakov, S.V. Vanjashin, A.Ju. Grebeshkov — Samara: Volga Region State University of Telecommunications and Informatics, 2015. — 135 p. [in Russian]

13. Rentjuk V.K. Kratkij putevoditel' po besprovodnym tehnologijam «Interneta veschej». Chast' 2. Blizhnij radius dejstvija [A short guide to wireless technologies of the Internet of Things. Part 2. Short range] / V.K. Rentjuk // Control Engineering Russia. — 2018. — 1. [in Russian]

14. Zhihao W. Towards IP geolocation with intermediate routers based on topology discovery / W. Zhihao, L. Hong, L. Qiang et al. // Cybersecurity. — 2019. — 2.

15. Saenko I. Abnormal traffic detection in networks of the internet of things based on fuzzy logical inference / I. Saenko, I. Kotenko // Institute of Electrical and Electronics Engineers Inc. — 2015. — 18.

16. Patap U. Average state estimation in presence of outliers / U. Patap, C. Canudas-de-Wit, F. Garin // IEEE Conference on Decision and Control (CDC). — 2020. — 59.

17. Alanazi M. Anomaly Detection for Internet of Things Cyberattacks / M. Alanazi, A. Aljuhani // Tech Science Press. — 2022. — 72(1).

18. Thilakarathne N.N. Security and Privacy Issues in IoT Environment / N.N. Thilakarathne // International Journal of Engineering and Management Research. — 2020. — 10(1).

19. Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things — Introduced 2016-05-31. — Italy: Request for Comments, 2016.— 61 p.

20. Jones M.B. Using RSA Algorithms with CBOR Object Signing and Encryption (COSE) Messages / M.B. Jones // Internet Engineering Task Force. — 2017. — RFC8230.

21. Dagle J.E. Cyber-physical system security of smart grids / J.E. Dagle // IEEE PES Innovative Smart Grid Technologies (ISGT). — 2012. — 1.

22. Dovgal' V.A. Problemy i zadachi bezopasnosti intellektual'nyh setej, osnovannyh na Internete Veschej [Security problems and challenges of smart networks based on the Internet of Things] / V.A. Dovgal', D.V. Dovgal' // Quarterly peer-reviewed, refereed scientific journal "Bulletin of ASU". — 2017. — 4(211). [in Russian]